ontinet.com

eset



Protegemos su mundo digital

NOD32
antivirus system

Eset NOD32 Antivirus para MS Exchange Server

Instalación

ESET, spol. s r. o.

Última revisión en inglés: 6 de junio de 2007.
Traducción y adaptación al español: Ontinet.com, S.L., agosto de 2007.

Indice

Introducción

ESET NOD32 Antivirus para MS Exchange Server es una nueva versión del antivirus ESET NOD32, diseñada para analizar el tráfico de mensajes de correo electrónico administrado por los servidores MS Exchange.

Entre las diferencias más importantes entre ESET NOD32 y ESET NOD32 para MS Exchange, encontramos la inclusión de un módulo denominado ***XMON***, y la ausencia de los módulos ***IMON*** y ***EMON***.

Este documento describe el módulo XMON. Para su mejor comprensión, le recomendamos la lectura previa de la **Ayuda y Manual del Usuario**, disponible en **http://www.nod32-es.com/download/manual_tec2.htm**.

Al igual que en la versión 2.71 de ESET NOD32, el módulo XMON proporciona protección antivirus para MS Exchange Server en dos variedades:

- Una versión 32-bit para MS Exchange Server 5.5 Service Pack 3 o superior, 2000 Service Pack 1 o superior, y 2003 (xmon.dll).

- Una versión 64-bit para MS Exchange Server 2007 (xmon64.dll).

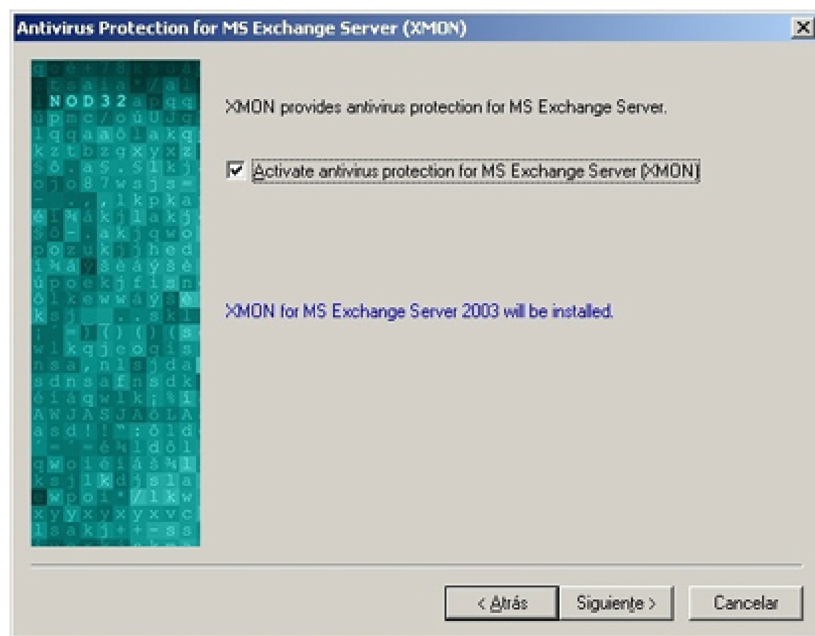
El módulo XMON verifica los correos electrónicos de MS Exchange Server a través de su interfaz antivirus VSAPI, o mediante las funcionalidades instrumentadas en NOD32 Control Center.

Instalación

Si está ejecutando una versión anterior de ESET NOD32 para MS Exchange Server, la nueva aplicación puede ser instalada sobre esta, si se trata de una versión 2.0 o posterior.

El asistente de instalación lo guiará durante este proceso. Sólo tiene que seguir las instrucciones que aparecen en pantalla.

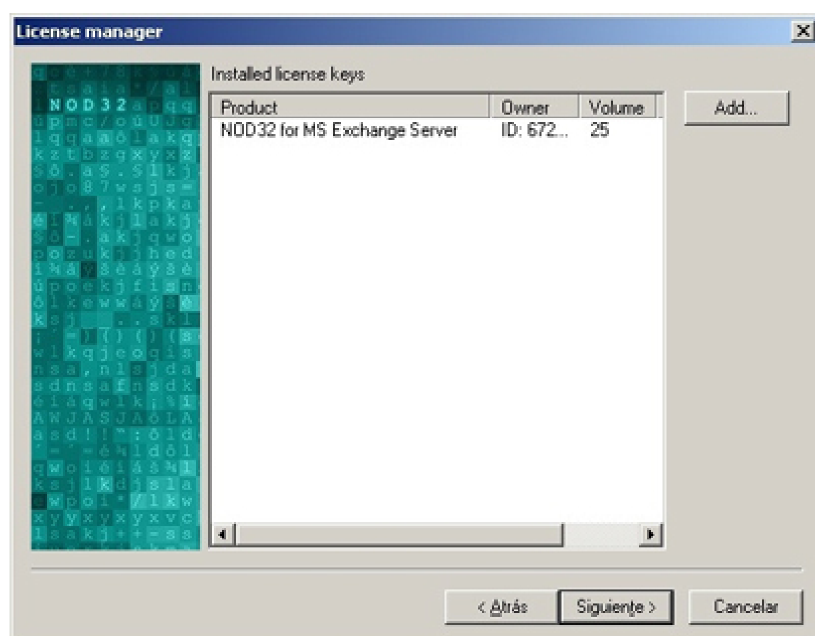
Durante la instalación de esta aplicación podrá optar por activar el módulo XMON ahora, o posteriormente y después de finalizado el proceso, desde dentro de NOD32 Control Center, XMON.



Marque la opción ***Activate antivirus protection for MS Exchange Server (XMON)*** (Activar la protección antivirus para MS Exchange Server) si desea su inmediata protección.
A continuación, pulse en el botón **Siguiente**.

Para activar el servicio XMON, necesitará el archivo de licencia entregado por su distribuidor autorizado, quien se lo proporcionará después de adquirida la licencia de uso.

Una vez recibido dicho archivo de licencia, pulse en el botón ***Add*** (Agregar) para incorporarla a la lista.



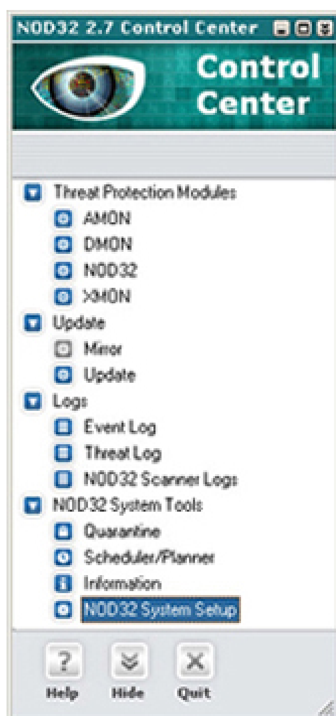
Activación de XMON

Si no ha activado la protección antivirus de ESET NOD32 para MS Exchange Server durante la instalación, puede realizar esta acción a través de la opción ***License Manager*** (Administrador de licencias).

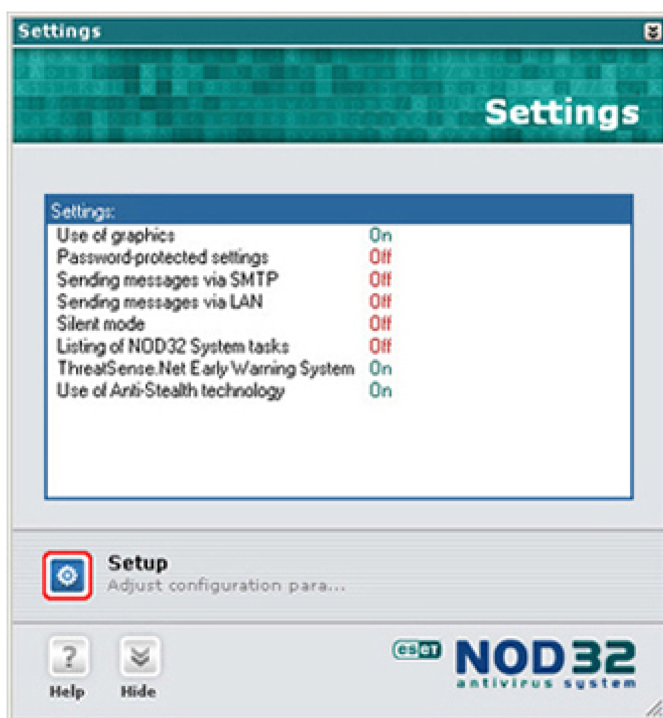
1. Abra ***ESET NOD32 Control Center***.

2. Localice el conjunto ***ESET NOD32 system tools*** (Herramientas del sistema NOD32).

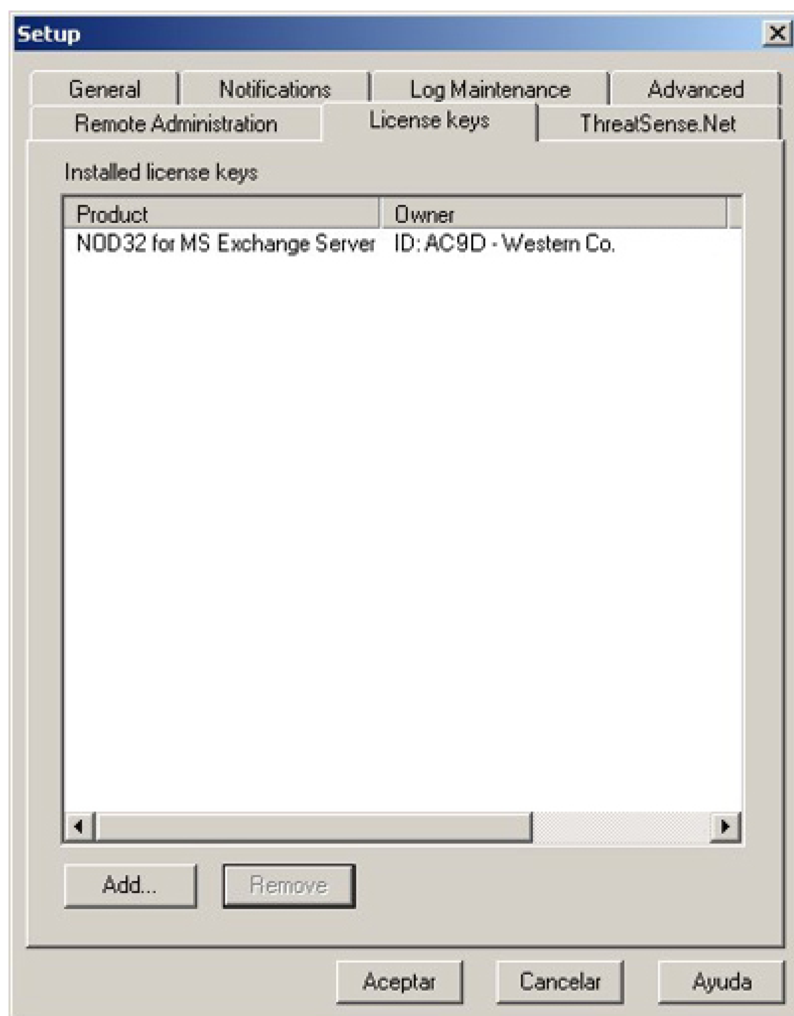
3. Pulse sobre ***ESET NOD32 system setup*** (Configuración del sistema NOD32).



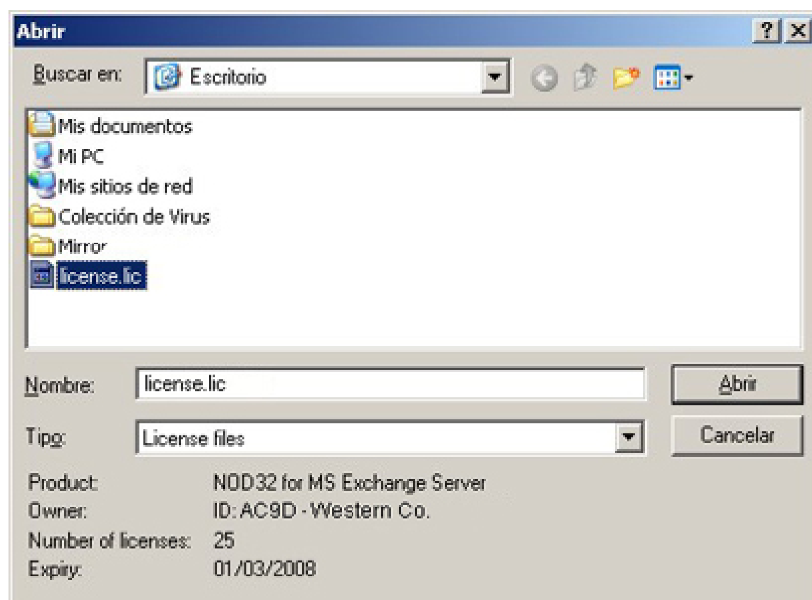
4. En la ventana de la derecha, presione el botón ***Setup*** (Configuración).



5. Pulsando en el botón ***Add*** (Agregar), cuando el archivo de licencia esté incluido en la pestaña ***License Keys*** (Claves de licencia), XMON se activará.



6. Al seleccionar el archivo de licencia, se visualizará información sobre la misma.



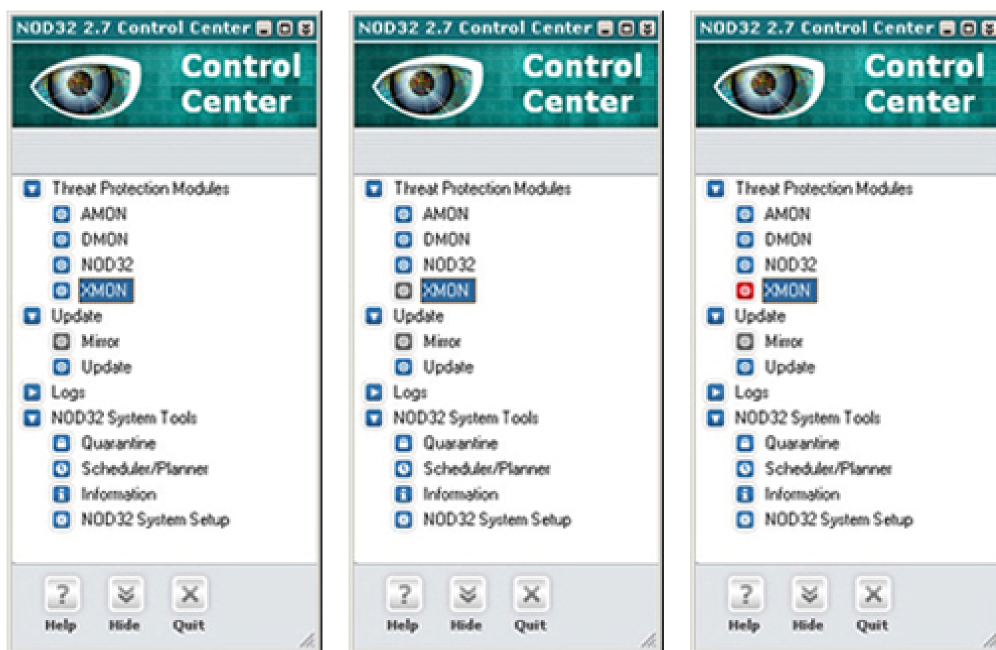
XMON: Ventana principal

Para visualizar la ventana principal de XMON, abra ***NOD32 Control Center*** y despliegue el grupo ***Threat Protection Modules*** (Módulos de protección) para localizar su respectivo icono.

- Si el icono de XMON está de color ***azul***, significa que el mismo se encuentra operativo.

- Si en cambio se visualiza de color ***gris***, indica que el servidor MS Exchange no está presente en el ordenador local, o la versión instalada de este sistema operativo no es compatible con XMON.
  También puede verse de color gris cuando el módulo no está activado (no se ha configurado o la licencia ha caducado). En estos casos, XMON no podrá analizar los mensajes de correo electrónico.

- Si el icono de XMON está de color ***rojo***, implica que el módulo no está habilitado.
  Para activarlo, pulse sobre dicho icono y, en la ventana principal de XMON (se abre a la derecha), marque la casilla ***NOD32 for MS Exchange (XMON) Enabled*** (Activar NOD32 para MS Exchange - XMON).



Pulse en el icono de XMON y a la derecha se abrirá la ventana principal del módulo XMON.



La ventana principal de XMON muestra la cantidad de elementos analizados, infectados y desinfectados, considerándose que un elemento es equivalente a cada mensaje de correo electrónico y sus archivos adjuntos.
Esta ventana también exhibe la versión de MS Exchange que se está ejecutando en el servidor local, y la versión de la base de datos de firmas de virus, con la fecha de última actualización entre paréntesis.

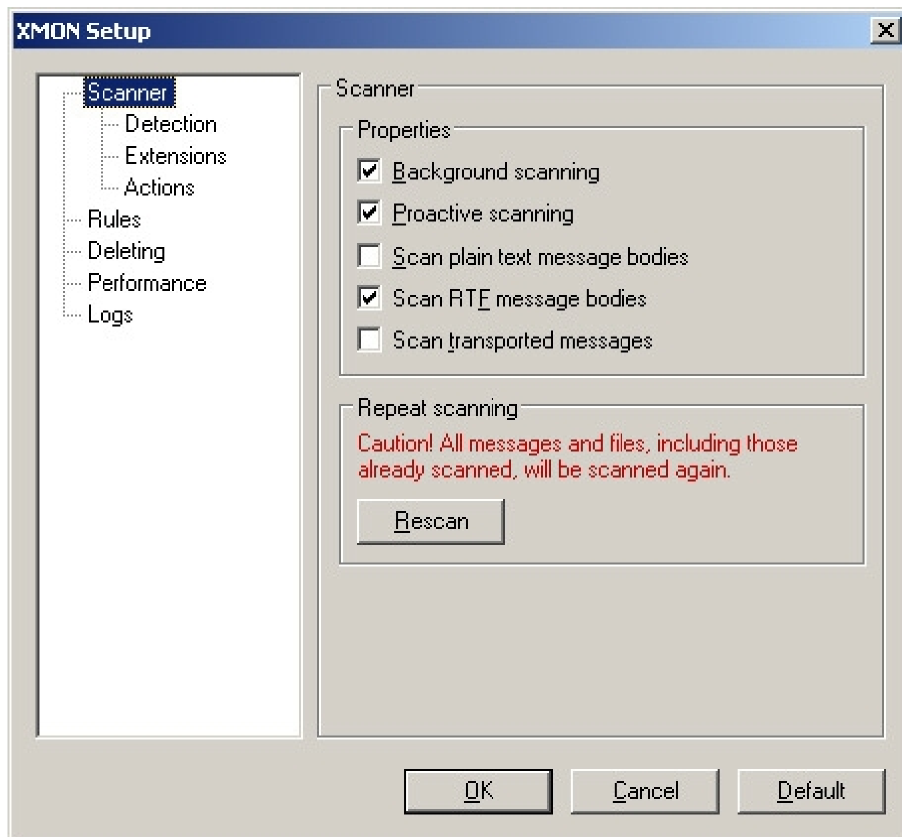
- ***NOD32 for MS Exchange (XMON) Enabled***
  (Activar NOD32 para MS Exchange - XMON)

  Es la casilla para activar XMON.
  Márquela para habilitar XMON, y desmárquela para desactivarlo.
  Antes de realizar esta última acción, XMON le solicitará que confirme su desactivación.
  Si realmente desea cerrar XMON, pulse sobre ***Yes*** (Si).



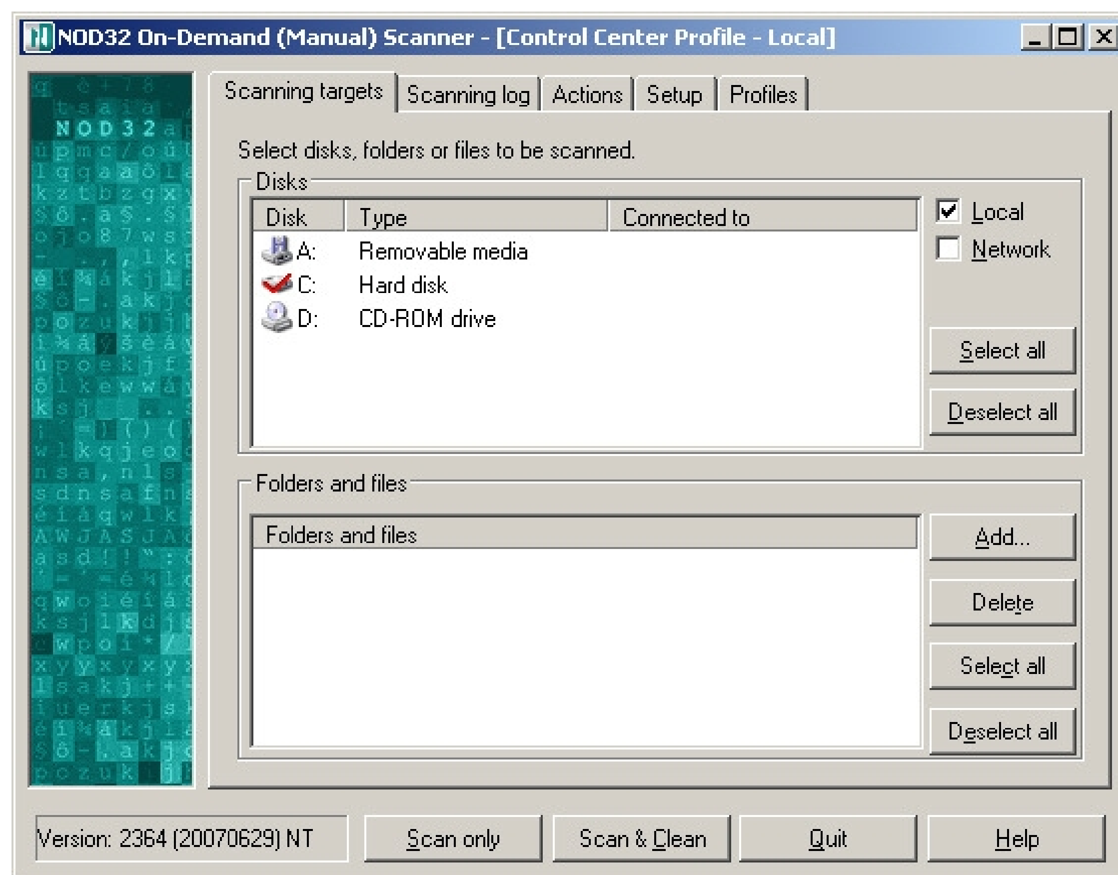
- ***Setup***
  (Configuración)

  Pulsando en el botón ***Setup***, le permitirá acceder a la configuración y modificar los valores por defecto de XMON.



- ***Run NOD32***
  (Ejecutar NOD32)

  Activa el análisis a petición del usuario de ESET NOD32 Antivirus.

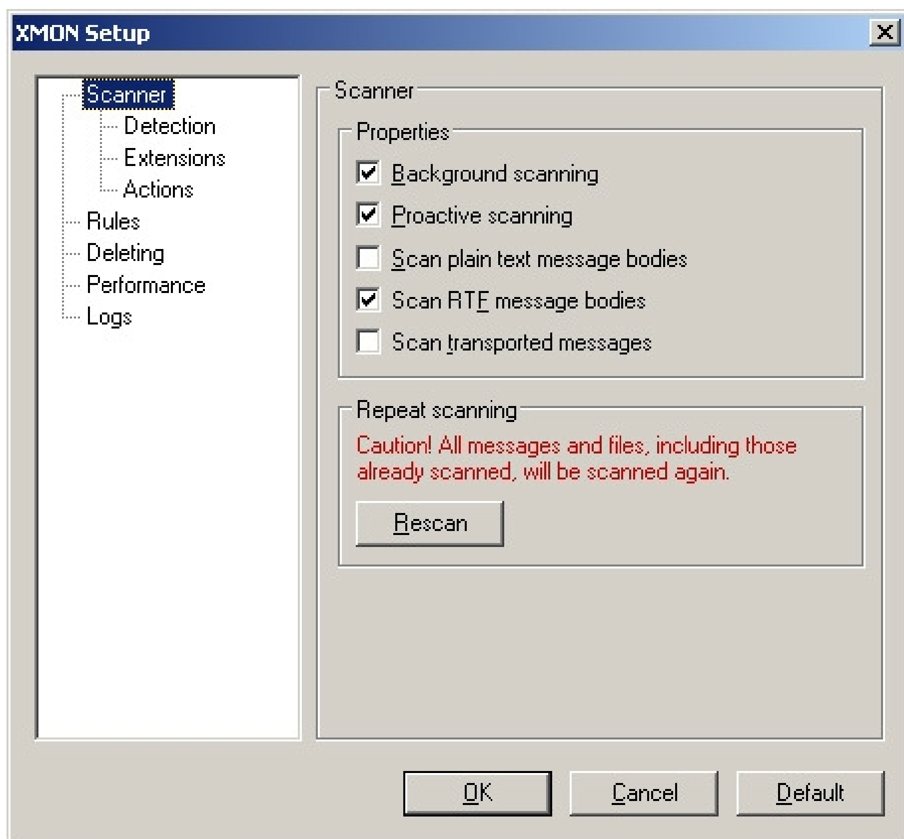


MS Exchange Server se comunica con el analizador antivirus utilizando la base de datos del registro de sistema.
Esta se verifica aproximadamente una vez por minuto.
Activar o desactivar XMON, así como cualquier otro cambio realizado en su configuración, podría demorar alrededor de un minuto para entrar en vigencia.

Setup (Configuración)

El lado izquierdo de la ventana de configuración de XMON, muestra ocho áreas, cuyos parámetros pueden ser modificados por el usuario, para adecuarlos a sus preferencias y necesidades.

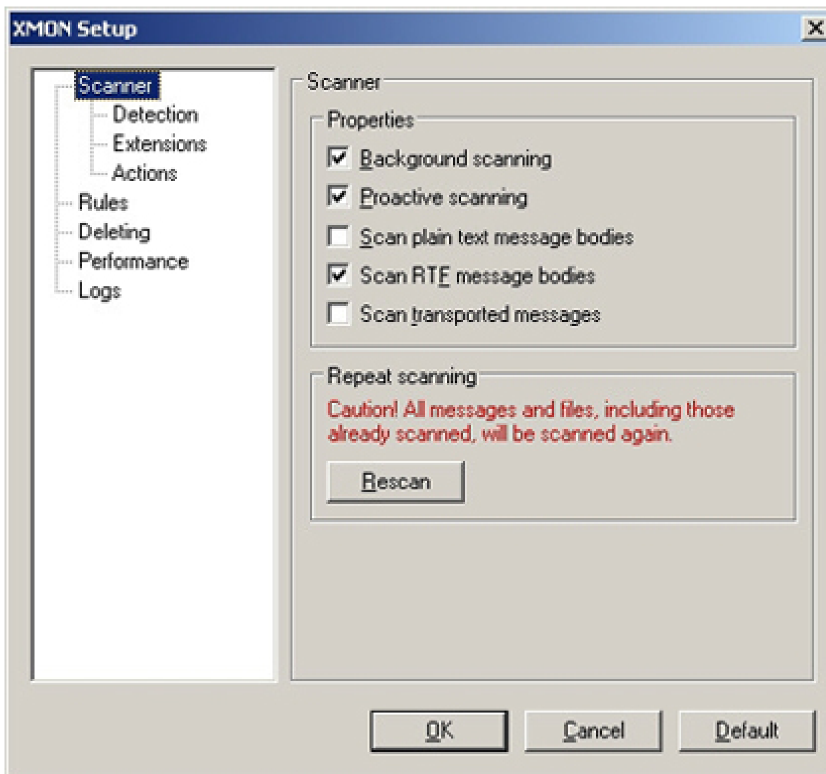
Al pulsar en un título de la izquierda, a la derecha, se visualiza el detalle de las opciones disponibles.



El servidor MS Exchange, verifica la configuración del módulo XMON a cada minuto, de modo que los nuevos valores de los parámetros de XMON entran en vigencia después de unos pocos segundos.

Scanner (Características del análisis)

En esta sección, se pueden configurar los parámetros relacionados con el análisis antivirus.



1. ***Background scanning***
(Análisis en segundo plano)
Si está marcada esta opción, todos los mensajes se analizarán en segundo plano. XMON mantiene un registro de los mensajes que verificó, y de la versión de la base de datos de virus que utilizó. Si un usuario intenta abrir un mensaje que no ha sido analizado con la última versión de la base de virus, XMON lo verifica antes de mostrarlo en su aplicación cliente de correo electrónico.
El análisis en segundo plano sirve para ahorrar tiempo, pues cuando el usuario abre un mensaje proveniente del servidor Exchange, este ya ha sido analizado. Al analizar la base de datos guardada en modo diario, la velocidad del sistema podría disminuir. En este caso, recomendamos utilizar análisis programados, que se ejecuten cuando el ordenador no esté siendo utilzado. Con el análisis programado activado, esta opción debe ser desactivada.

2. ***Proactive scanning***
(Análisis proactivo)
Los nuevos mensajes entrantes se analizan en el orden en que se reciben.
Si esta casilla está marcada, y un usuario abre un mensaje que todavía no fue verificado, este se analizará antes que el resto de los mensajes que están en cola de espera.

3. ***Scan plain text message bodies***
(Analizar el cuerpo de los mensajes cuyo formato es texto plano)
Esta opción habilita la verificación de mensajes que han sido enviados en texto plano.

4. ***Scan RTF message bodies***
(Analizar el cuerpo de los mensajes RTF)
Esta opción habilita el análisis de los mensajes en formato ***RTF*** (*Rich Text Format*, Formato de texto enriquecido).
El cuerpo de estos mensajes podría contener macrovirus.

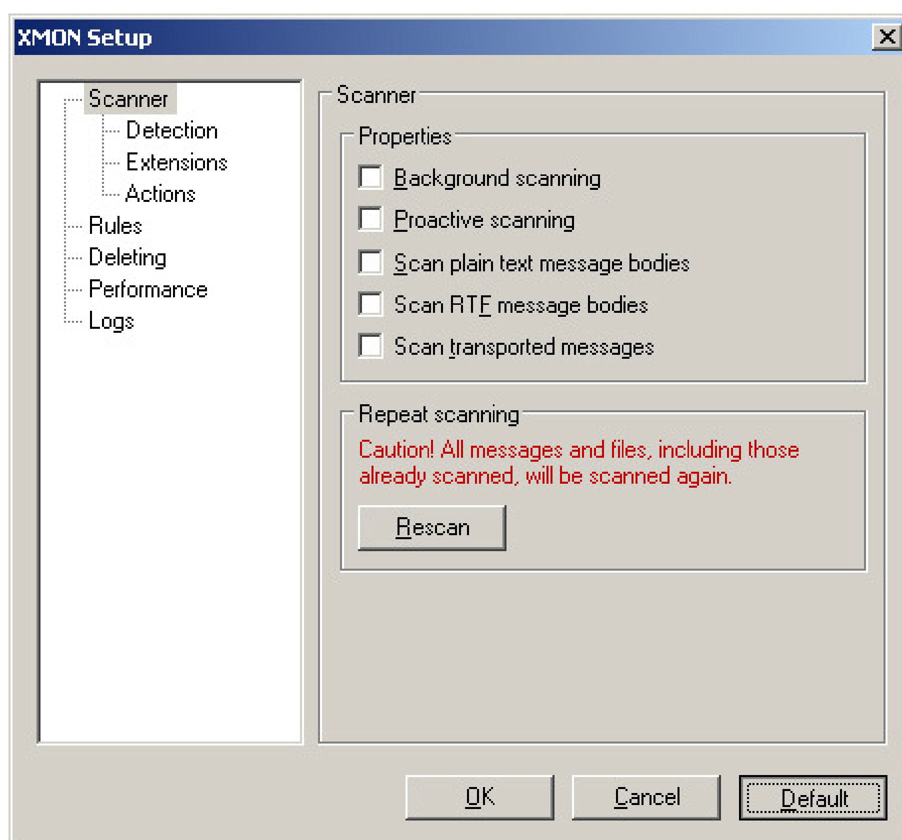
5. ***Verify file size***
(Verificar tamaño de los archivos)
Cuando está marcada esta opción, XMON determinará el tamaño preciso de los archivos adjuntos en los mensajes de correo electrónico que pasan por el servidor Exchange, sin tener en cuenta el tamaño que indica este último. El servidor sólo calcula un tamaño aproximado de los archivos adjuntos, para los mensajes codificados.
Determinar el tamaño exacto de los archivos adjuntos podría disminuir la velocidad del proceso de análisis, pero aumenta la precisión de la detección de virus.

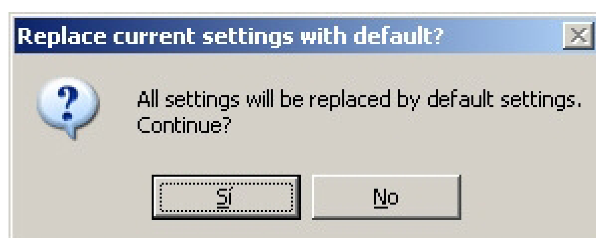
6. ***Scan transported messages***
   (Analizar mensajes transportados)
   Al marcar esta opción, XMON analizará también los mensajes que no están guardados en el servidor local de MS Exchange, y que son distribuidos a otros servidores de correo, utilizando el servidor local MS Exchange. El servidor MS Exchange puede estar definido como una puerta de comunicaciones (*Gateway*) y utilizado justamente para esto.

7. **Botón *Rescan***
   (Analizar nuevamente)
   Cuando está marcada esta opción, XMON analiza también los mensajes que no están guardados en el servidor MS Exchange local, y que son entregados a otros servidores de correo electrónico a través de este.

8. **Botón *Repeat scanning***
   (Analizar nuevamente)
   Al pulsar sobre este botón, todos los mensajes guardados en el servidor MS Exchange local se analizan nuevamente. Con cada actualización de la base de datos de virus, XMON también analiza todos los mensajes almacenados en el servidor local.

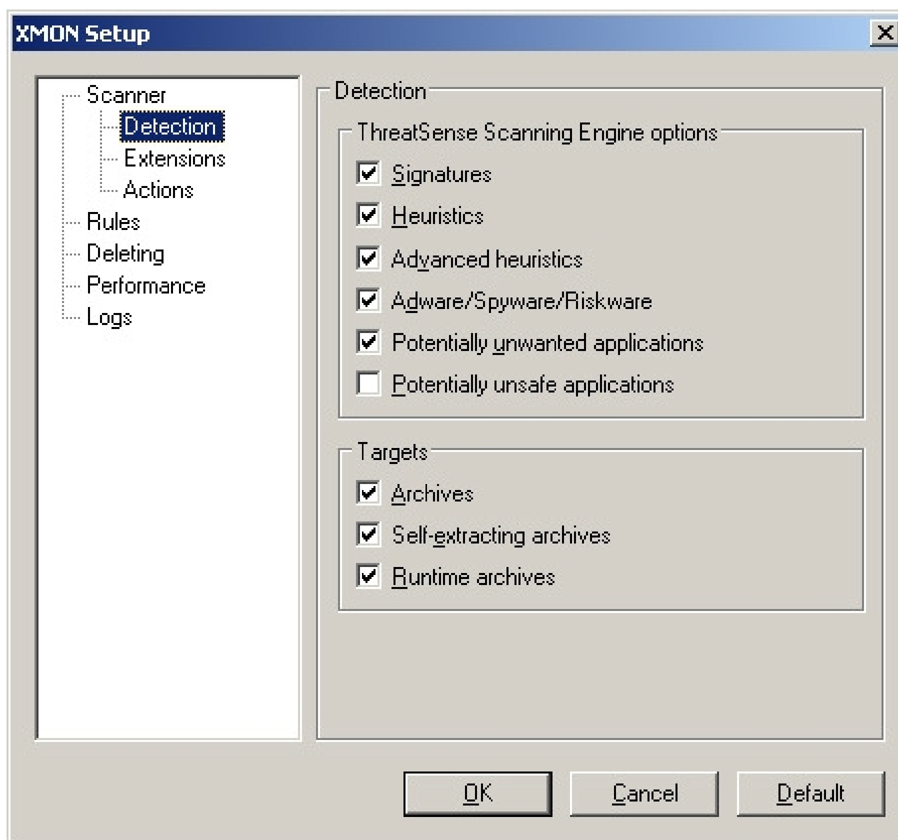
9. **Botón *Default***
   (Predeterminado)
   Al presionar este botón, todas las propiedades de la sección ***Scanner*** se configuran con los valores predeterminados. Antes de ejecutar esta acción, aparecerá una ventana de advertencia, que permite confirmar o cancelar la tarea solicitada. Al pulsar ***Yes*** (Si), se asignarán los valores configurados por defecto.





Detection (Detección)

Esta sección contiene la configuración de los métodos de detección.



1. Las opciones dentro de ***ThreatSense Scanning Engine options*** (Opciones de análisis a través de la tecnología ThreatSense) permiten configurar los métodos de detección de infiltraciones utilizados en el módulo XMON.
   Para obtener el nivel máximo de seguridad, marque todas las casillas.

   1. ***Signatures***
      (Firmas de virus)
      Cuando esta opción está marcada, XMON utiliza la detección de infiltraciones basada en firmas.

   2. ***Heuristics***
      (Heurística)
      Cuando está marcada esta opción, XMON utiliza el método basado en heurística para la detección de infiltraciones (análisis del contenido del archivo y su posible comportamiento).

   3. ***Advanced Heuristics***
      (Heurística avanzada)
      Cuando está marcada esta opción, XMON usa heurística avanzada para la detección de infiltraciones.
      Esta técnica es un conjunto de métodos heurísticos exclusivo, que puede detectar los gusanos de Internet más peligrosos.

   4. ***Adware / Spyware / Riskware***
      (Publicidad no solicitada / Programas espía / Aplicaciones peligrosas)
      Cuando esta opción está marcada, XMON también detecta este tipo de códigos maliciosos.

   5. ***Potentially unwanted applications***
      (Aplicaciones potencialmente indeseables)
      Las aplicaciones potencialmente peligrosas no necesariamente tienen fines maliciosos, pero podrían afectar el rendimiento del ordenador.
      Este tipo de programas solicitan el consentimiento del usuario para ser instalados, y cuando están presentes en el ordenador, el sistema suele presentar un comportamiento distinto al que tenía anteriormente.

6. ***Potentially unsafe applications***
   (Aplicaciones potencialmente peligrosas)
   Esta clasificación se utiliza para aplicaciones legítimas, e incluye programas como herramientas de acceso remoto, descifradores de contraseñas y registradores de pulsaciones de teclas.

2. Las opciones del sector ***Targets*** (Objetos a verificar), permiten configurar qué tipos de archivos se analizarán:

   - ***Archives***
     (Archivos comprimidos)

   - ***Self-extracting archives***
     (Archivos comprimidos auto extraíbles)

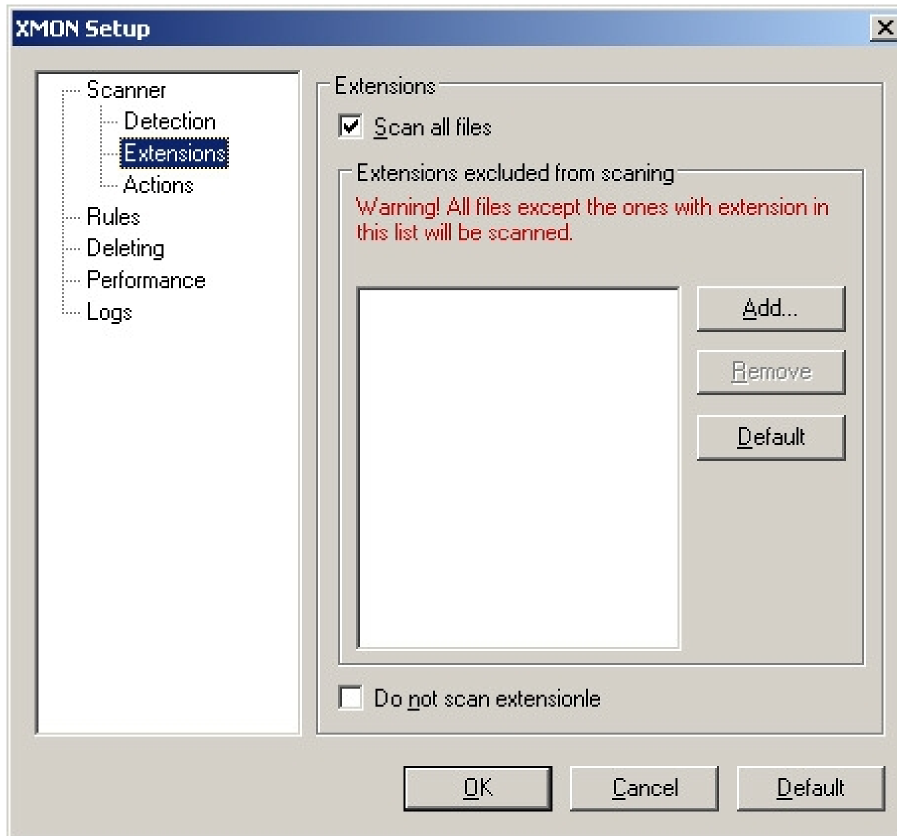
   - ***Run-time archives***
     (Archivos comprimidos en tiempo de ejecución).
     Al analizar archivos comprimidos, el procedimiento de verificación consume más tiempo, porque cada elemento debe ser abierto para su control.

Extensions (Extensiones)

Esta sección permite configurar qué tipo de archivos debería incluirse en el análisis de virus, filtrándolos por su extensión.

Se recomienda utilizar los parámetros predefinidos, y permitir que XMON verifique todas las extensiones posiblemente peligrosas.

La verificación de todas las extensiones posibles podría disminuir el rendimiento del ordenador, y el usuario deberá establecer el parámetro más adecuado a su particular entorno de trabajo.

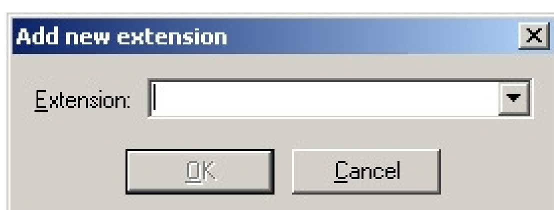


1. ***Scan all files***
   (Analizar todos los archivos)
   Cuando esta opción está marcada, XMON analizará todos los tipos de archivo que se encuentren adjuntos en los mensajes de correo electrónico.

2. Si la opción ***Scan all files*** está marcada, la lista de tipos de archivo que aparece en el sector ***Extensions excluded from scanning*** (Extensiones excluidas del análisis) mostrará qué extensiones serán excluidas del análisis, y no las que se incluirán en él.

   1. ***Add***
      (Agregar)
      Permite añadir una nueva extensión de archivo a la lista.
      Se pueden utilizar caracteres alfanuméricos y comodines tales como “?” (que representa un carácter al azar) o “*” (que representa un orden aleatorio de caracteres).

      Al pulsar este botón, aparecerá una nueva ventana.
      Escriba la nueva extensión (por ejemplo: ***ehg***, sin el punto previo habitual) y pulse en el botón ***OK*** (Aceptar).



2. ***Remove***
   (Eliminar)
   Elimina de la lista la extensión seleccionada.

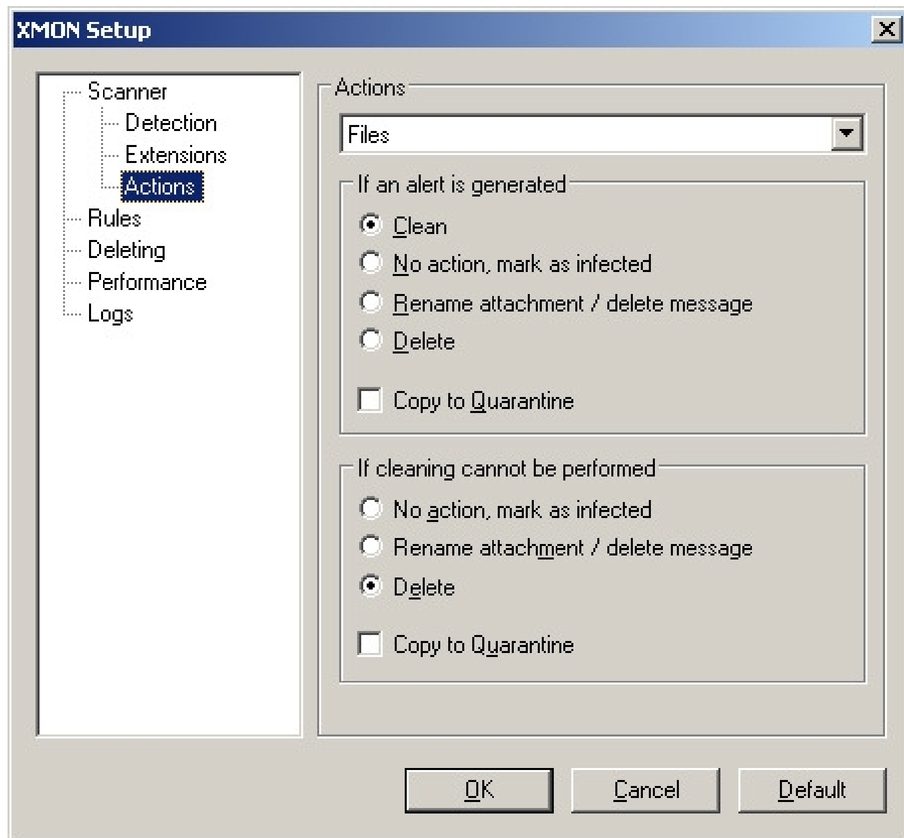
3. ***Default***
   (Predeterminado)
   Restablece la lista de extensiones predefinida.

4. ***Do not scan extension-less files***
   (No analizar archivos sin extensión)
   Excluye del análisis los archivos sin extensión.

Actions (Acciones)

Esta sección permite seleccionar la acción o acciones que deberían ejecutarse cuando se detecta un virus.

En la sección ***Detection*** (Detección) se habilitan los tipos de archivos que posteriormente se visualizarán en esta sección ***Actions*** (Acciones).
Seleccione un tipo de archivo en el menú desplegable y defina la configuración.
Seleccione otro tipo de archivo en el mismo menú desplegable, y defina los parámetros para el siguiente tipo de archivo.
Continúe hasta terminar de establecer los valores para cada tipo de archivo.



1. La opciones de ***If an alert is generated*** (Si un alerta es generado) permite elegir la acción que debería ejecutarse cuando se detecte un virus.

    1. ***Clean***
       (Desinfectar)
       XMON intentará limpiar el virus del archivo infectado.
       Si no fuera posible, se ejecutará la acción seleccionada en ***If cleaning cannot be performed*** (Si es imposible desinfectar).

    2. ***No action, mark as infected***
       (Sin acciones, informar)
       Cuando esta seleccionada esta opción, el servidor Exchange es notificado sobre la infección y el usuario no puede abrir el archivo adjunto infectado.

    3. ***Rename attachment / delete message***
       (Modificar nombre del adjunto/ Borrar mensaje)
       XMON cambia la extensión del archivo adjunto, para que no puede ser abierto o ejecutado.
       Si su cuerpo contiene un virus, el mensaje será eliminado.

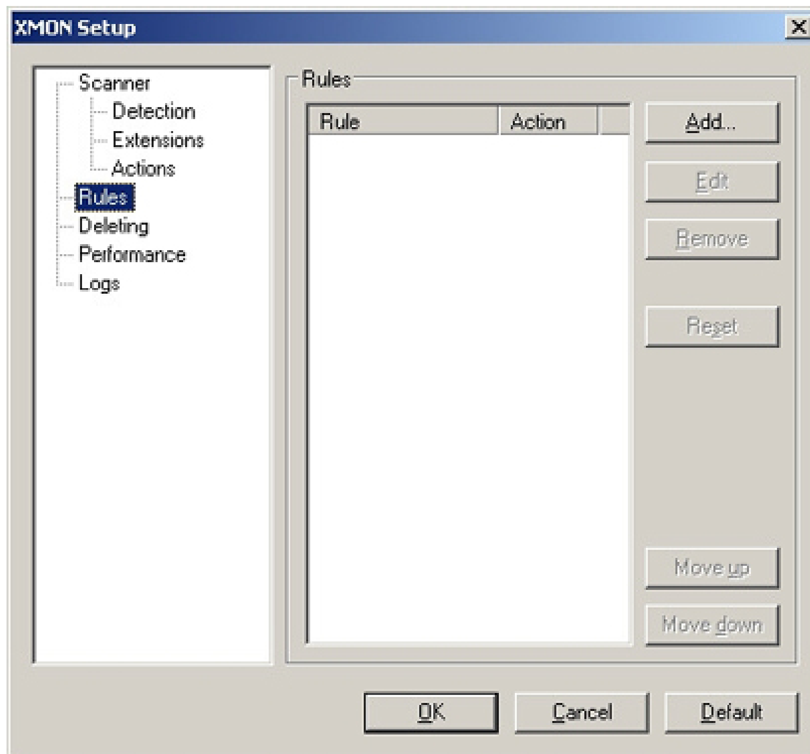
    4. ***Delete***
       (Eliminar)
       XMON borra el mensaje infectado o el archivo adjunto si solo este último está infectado.
       El proceso de eliminación puede personalizarse en la sección ***Deleting setting*** (Configuración de borrado)

5. ***Quarantine***
   (Copiar a Cuarentena)
   Cuando está marcada esta opción, los mensajes infectados se guardarán en Cuarentena, donde son convertidos en inocuos.
   Estos mensajes pueden ser analizados y limpiados posteriormente, utilizando una base de firmas de virus más reciente.

2. La configuración de ***If cleaning cannot be performed*** (Si es imposible desinfectar) se activa si está marcada la opción ***Clean*** (Desinfectar) del sector anterior.
   Algunas de las infecciones no pueden ser eliminadas porque XMON no tiene definido un procedimiento de limpieza para ellas, o porque el contenido es solamente el virus.
   Generalmente, este último caso es el más frecuente.
   Las opciones de este sector permiten seleccionar qué acción debería ejecutarse cuando falla el intento de limpiar un virus.

Rules (Reglas)

Esta sección permite configurar reglas detalladas para administrar distintos tipos de archivo.
Si hay más de una regla para un mismo tipo de archivo, entonces se aplicará la que figure antes en la lista.



Las reglas tienen mayor prioridad que la configuración de extensiones definida en la sección ***Extensions settings*** (Configuración de extensiones).
Esto significa que primero, cada archivo se compara con las reglas existentes, y solo será analizado si no encuentra instrucciones correspondientes a él, o si estas dicen expresamente que debe ser verificado.

La cantidad de reglas aplicadas se muestra en la columna ***Action*** (Acciones).

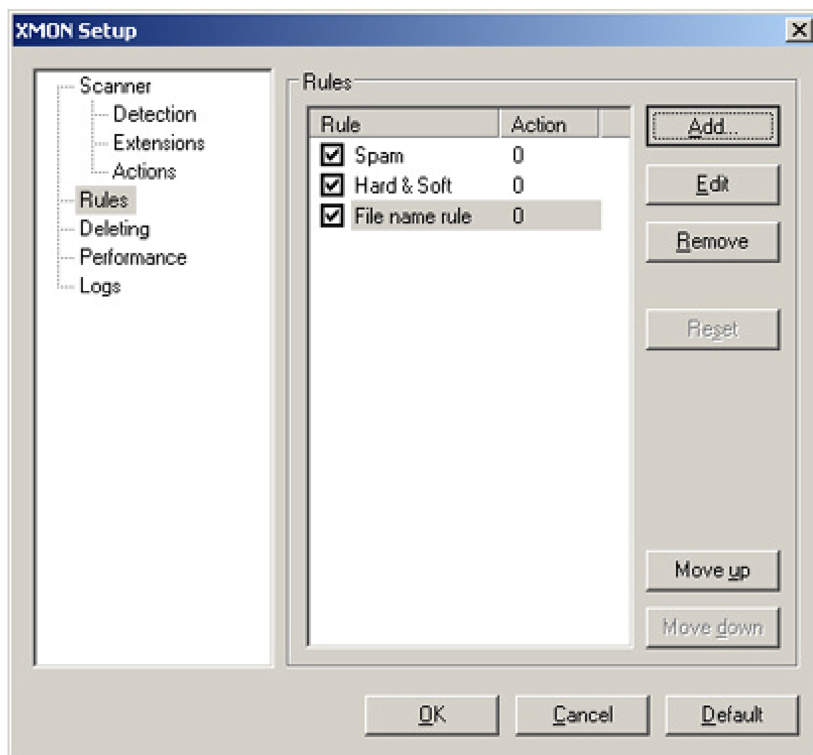
1. **Botón *Add***
   (Agregar)
   Permite agregar una regla nueva.

2. **Botón *Edit***
   (Editar)
   Permite modificar la regla seleccionada.

3. **Botón *Move up***
   (Subir un nivel)
   Sube la regla seleccionada un nivel, y aumenta su prioridad.

4. **Botón *Move down***
   (Bajar un nivel)
   Baja la regla seleccionada un nivel, y disminuye su prioridad.

Para agregar una regla, presione el botón ***Add*** (Agregar). Se abrirá un asistente que lo guiará a través del proceso.



1. En la primera ventana, hay que seleccionar el criterio que se utilizará para aplicar la regla.

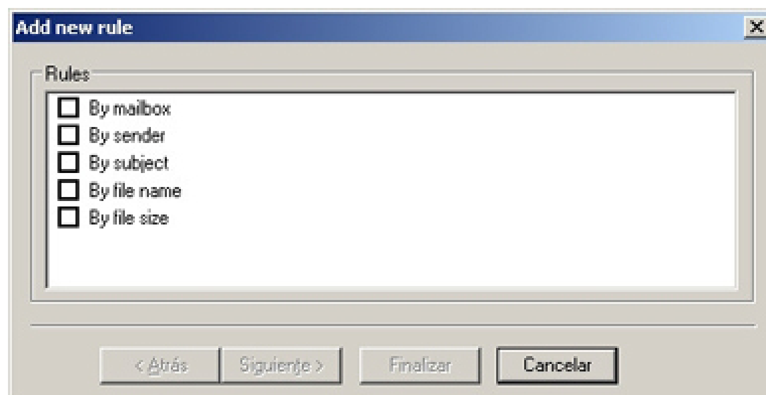
   1. ***By mailbox***
      (Por casilla de correo)
      La regla se aplica al nombre de una casilla de correo.

   2. ***By sender***
      (Por remitente)
      La regla se aplica a un mensaje enviado por el remitente seleccionado.

   3. ***By subject***
      (Por asunto)
      La regla se aplica a un mensaje con el asunto seleccionado.

   4. ***By file name***
      (Por nombre de archivo)
      La máscara de nombres permite elegir una determinada selección de archivos.

   5. ***By file size***
      (Por tamaño del archivo)
      Esta opción permite elegir archivos del tamaño especificado.



2. En la siguiente ventana, podrá marcar el grado de coincidencia con las palabras introducidas como filtro.

   1. Si selecciona la opción ***By message*** (Por mensaje) o ***By subject*** (Por asunto), y no activa la opción ***Match whole words*** (Coincidir palabras completas), en las cadenas de caracteres introducidas solo será necesario completar una parte del texto.

      Si la opción ***Match case*** (Coincidir mayúsculas y minúsculas) no está marcada, no se hará distinción entre letras mayúsculas o minúsculas.

      Al utilizar caracteres especiales no alfanuméricos, se deben utilizar paréntesis y comillas.
      También se pueden crear condiciones, utilizando los operadores lógicos ***AND*** (y), ***OR*** (o), ***NOT*** (negación).

      Add new rule
      Mailbox
      Conditions can be defined using logical operators AND, OR and NOT.
      When specifying multiple conditions, you can use parenthesis and speech marks.
      Admin
      Match whole words only
      Match case
      < Atrás | Siguiente > | Finalizar | Cancelar

      Si selecciona la opción ***By file name*** (Por nombre de archivo), en ***File name mask*** (Máscara de nombre de archivo) podrá especificar un criterio de selección de archivos, utilizando una máscara creada con caracteres alfanuméricos y comodines, como "?" y "*", por ejemplo: "*.VBS". La regla se aplicará a los archivos que coincidan con esta máscara. Para usar más de una máscara, solo hay que separarlas con punto y coma.

      Add new rule
      File name mask
      File name mask supports wildcards (* and ?).
      When specifying multiple masks, delimit them with a semicolon.
      Name_number_???.*
      < Atrás | Siguiente > | Finalizar | Cancelar

   2. Si escoge filtrar por la opción ***By file size*** (Por tamaño del archivo), en ***File size limit*** (Tamaño de archivo límite) podrá especificar un tamaño límite para los archivos adjuntos. La regla se aplicará a todos aquellos que excedan el valor definido.

      Add new rule
      File size
      The rule will be applied to all attachments with the size exceeding the defined value.
      Warning! Selecting a very low limit may cause the rule to be applied to all messages.
      File size limit 5 MB
      < Atrás | Siguiente > | Finalizar | Cancelar

3. En la siguiente ventana, la sección ***Action*** (Acción) permite determinar qué acciones deberían realizarse con los archivos que cumplen con el criterio de selección determinado en el paso anterior.

    1. ***Action settings to use for scanning***
    (Configuración de acciones al analizar):
    XMON analizará el tipo de archivo seleccionado en el menú desplegable, en busca de virus.

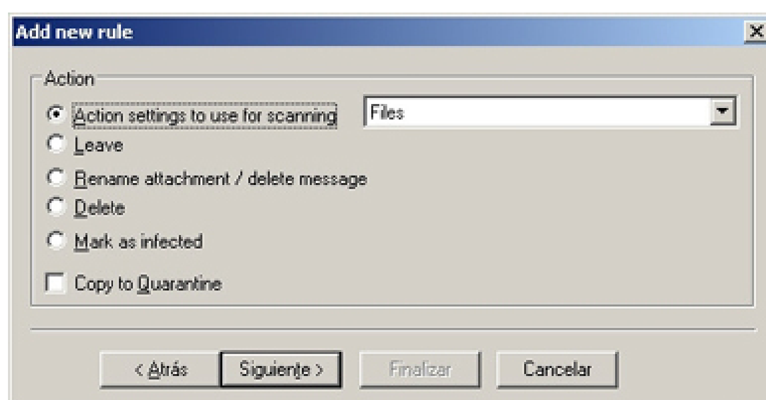
    2. ***Leave***
    (No ejecutar ninguna acción):
    XMON declarará que el mensaje está limpio.

    3. ***Rename attachment / delete message***
    (Modifcar nombre del archivo adjunto / borrar mensaje):
    XMON cambia la extensión del archivo para que no pueda ser abierto ni ejecutado.

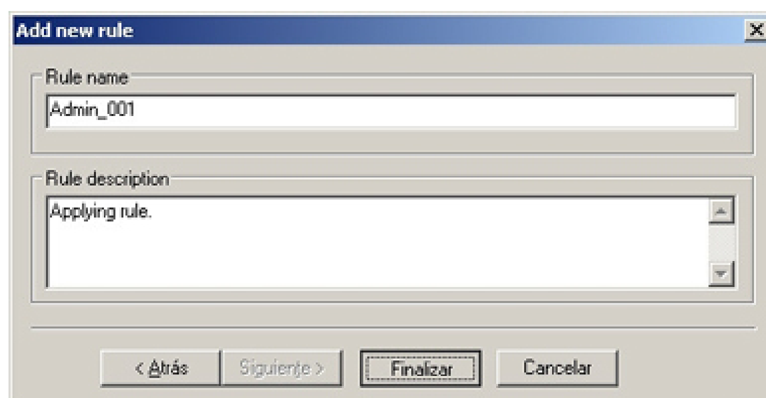
    4. ***Delete***
    (Eliminar):
    XMON elimina el mensaje seleccionado.

    5. ***Mark as infected***
    (Marcar como infectado)
    XMON marca el mensaje seleccionado como infectado.

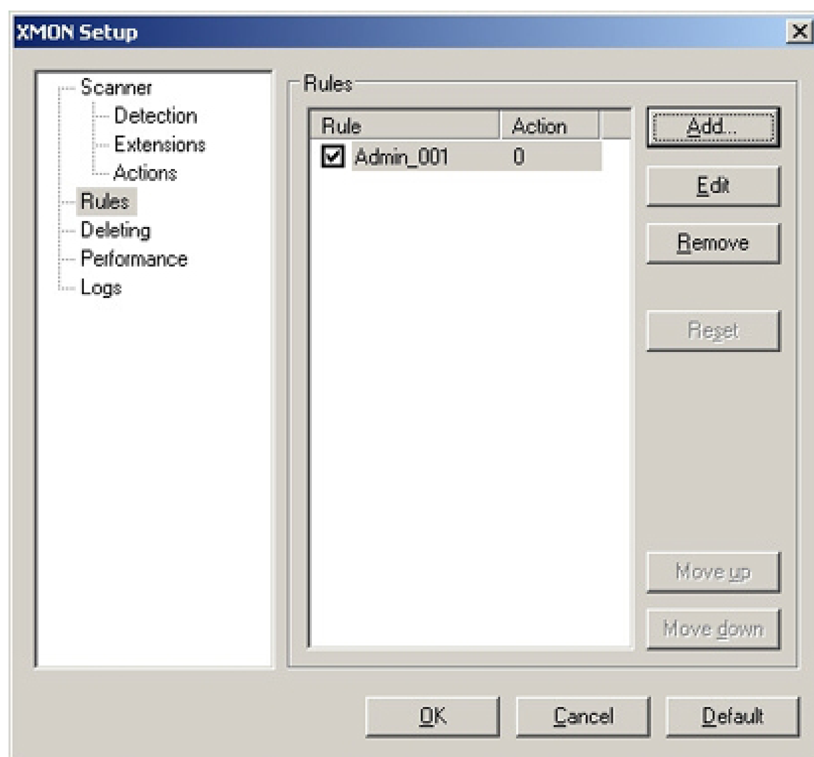
    6. ***Copy to Quarantine***
    (Copiar en Cuarentena)
    El mensaje seleccionado se guardará en Cuarentena.



4. Finalmente, hay que agregar el nombre de la regla y la descripción para que esta se guarde en el registro del servidor Exchange con una denominación descriptiva.

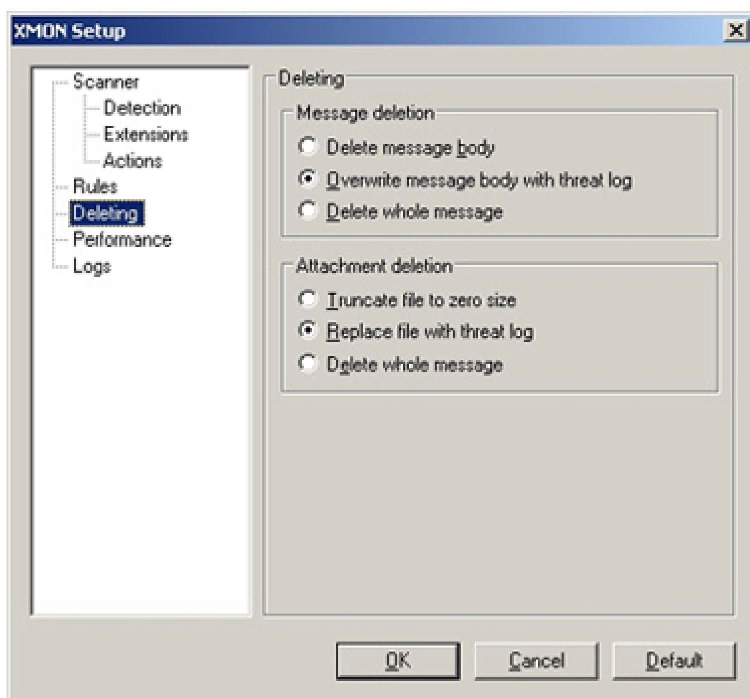


5. Las reglas creadas aparecerán en la lista de la ventana principal.



Deleting (Eliminación)

Esta sección permite determinar la acción que debería ejecutarse, cuando un mensaje o archivo adjunto se selecciona para su eliminación.



1. En el sector ***Messaging deletion*** (Eliminación de mensajes) se puede escoger qué acciones se tomarán cuando el mensaje completo ha sido marcado para su eliminación.

    1. ***Delete message body***
    (Eliminar cuerpo del mensaje)
    XMON borra el cuerpo del mensaje infectado. El destinatario recibirá el mensaje vacío, junto con los archivos adjuntos no infectados.

    2. ***Overwrite message body with threat log***
    (Sobrescribir el cuerpo del mensaje con información sobre la amenaza)
    XMON sobrescribe el cuerpo del mensaje con datos de la amenaza o la descripción de una regla.

    3. ***Delete whole message***
    (Eliminar mensaje completo)
    XMON borra el mensaje completo, incluyendo todos los archivos adjuntos.

2. Los parámetros de ***Attachment deletion*** (Eliminación de archivos adjuntos), permiten seleccionar qué acción debería ejecutarse con los archivos adjuntos cuando un mensaje se ha marcado para ser eliminado.

    1. ***Truncate file to zero size***
    (Truncar el archivo a tamaño nulo)
    XMON vacía el archivo, y deja que el destinatario vea su nombre y su tipo.

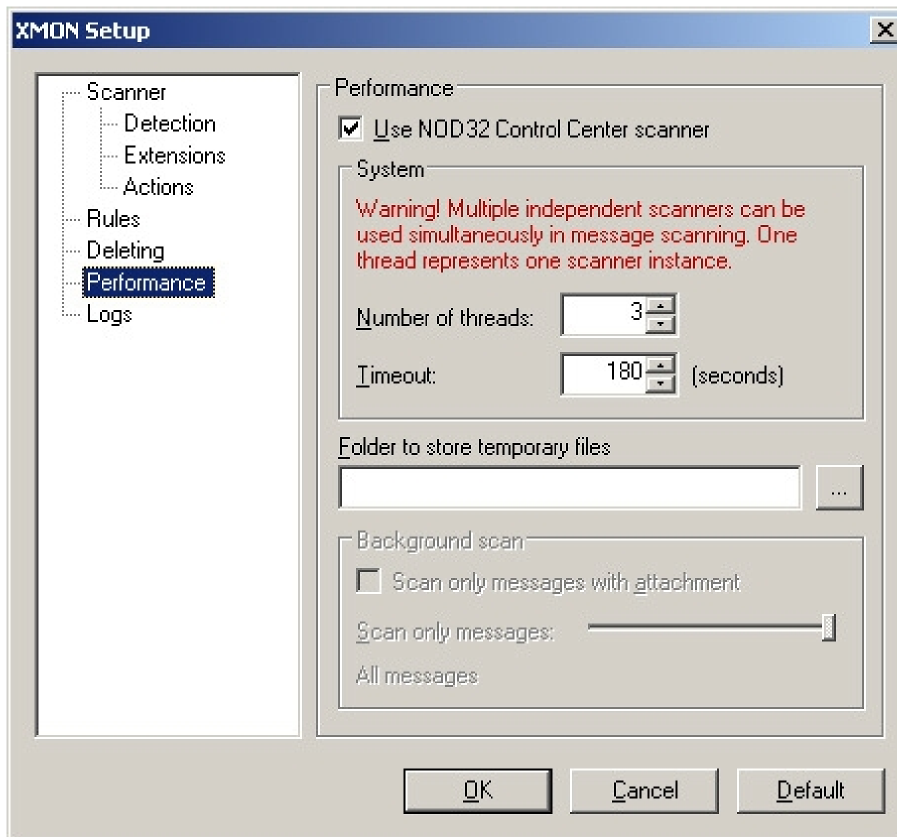
    2. ***Replace file with threat log***
    (Reemplazar el archivo con información sobre la amenaza)
    XMON reemplaza el archivo infectado con datos de la amenaza o la descripción de una regla.

    3. ***Delete whole message***
    (Eliminar mensaje completo)
    XMON borra el mensaje completo, junto con sus archivos adjuntos.

Si no se puede abrir la sección ***Deleting***, que aparece de color gris, significa que esta opción no es compatible con la versión de MS Exchange Server instalada en el ordenador.

Performance (Rendimiento)

Esta sección permite configurar los parámetros de rendimiento para XMON.



1. ***Use NOD32 Control Center scanner***
   (Utilizar el analizador de NOD32 Control Center)
   A diferencia de las versiones anteriores, que explícitamente usaban el corazón de análisis interno para verificar la existencia de virus, la versión 2.71 ofrece la opción de usar el centro de análisis externo también.
   En las versiones 32-bit de MS Exchange Server, esta característica es opcional, y se la puede seleccionar en esta sección.
   En la versión 64-bit de MS Exchange Server, solo es posible utilizar el centro de análisis externo. Por lo tanto, esta opción estará seleccionada por defecto, y no podrá modificarse.

2. ***Number of threads***
   (Cantidad de hilos o instancias)
   Este parámetro sirve para determinar cuántas instancias de ejecución deberían utilizarse para el análisis de virus.
   Una cantidad mayor de hilos en máquinas con multiprocesadores, podría incrementar la velocidad de análisis.
   El proveedor de MS Exchange Server recomienda aplicar la siguiente fórmula para determinar el número de hilos usados:
   Número de procesadores físicos elevado al cuadrado, más 1 = Cantidad de hilos o instancias simultáneas.

3. ***Timeout***
   (Límite de tiempo)
   Determina el intervalo de tiempo para ejecutar el análisis de virus.

4. ***Time limit***
   (Límite de tiempo), para Exchange 5.5
   Determina el intervalo de tiempo para ejecutar el análisis de virus.

5. ***Time limit***
   (Límite de tiempo), para Exchange 2000 y superiores
   Determina el límite de tiempo para analizar un archivo individual.

6. ***Folder to store temporary files***
   (Carpeta donde se guardarán los archivos temporales)
   Para obtener el mejor rendimiento, se recomienda configurar XMON para que guarde los archivos temporales en un disco físico diferente al que contiene el almacén de Exchange.
   Si no se especifica ninguna ruta, XMON utilizará la carpeta temporal del sistema para guardar estos archivos.

7. ***Background scan scope***
   (Alcance del análisis en Segundo plano)
   MS Exchange Server 2007 proporciona un método para afectar activamente el análisis antivirus en segundo plano.
   Por lo tanto, el módulo XMON de la versión 64-bit ofrece una opción para configurar el progreso y el rango de alcance de este tipo de análisis. Sin embargo, esta opción no está disponible en las versiones 32-bit de MS Exchange Server y el módulo XMON, por lo tanto los controles estarán desactivados y de color gris.

   1. ***Scan only messages with attachment***
      (Analizar solamente los mensajes con archivos adjuntos)
      Si está marcada esta casilla, el análisis en segundo plano solo verificará los mensajes que contengan archivos adjuntos. Esto también aliviará la carga general del sistema durante el análisis.
      Es necesario destacar que no todos los mensajes infectados contienen un archivo adjunto. Sin embargo, esto no disminuirá la protección de los mensajes en el almacén de MS Exchange Server, pues estos también son verificados cuando el usuario accede a ellos.

   2. **Barra de nivel *Scan only messages***
      (Analizar solamente los mensajes)
      Esta barra de nivel brinda otra posibilidad para reducir la carga general del sistema.
      Cuando esta está activada, solo se analizarán en segundo plano los mensajes según la fecha de recepción.

      Es posible elegir entre:

      - Analizar todos los mensajes, sin importar la fecha de recepción.

      - Analizar los mensajes recibidos el último año, los últimos 6 meses, los últimos 3 meses, el último mes o la última semana.

      Seleccionar el nivel de análisis en segundo plano apropiado, permitirá que los administradores de MS Exchange 2007 configuren el rendimiento del sistema según sus necesidades.
      En este caso, los mensajes que no estén incluidos en el intervalo de tiempo especificado, tampoco estarán desprotegidos pues también serán verificados cuando el usuario acceda a ellos.

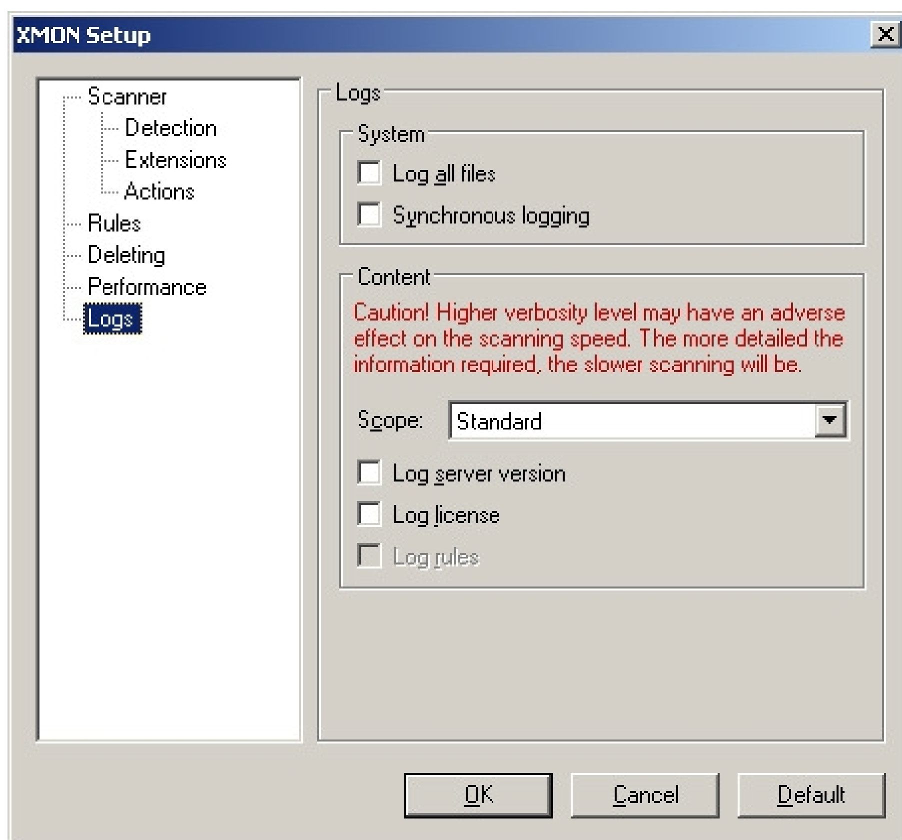
Debido a la elevada eficiencia de detección que brinda ESET NOD32 para MS Exchange Server, se recomienda:

1. Después de la instalación inicial de ESET NOD32 para MS Exchange Server, permitir que el análisis en segundo plano se ejecute sin restricciones.

2. Después de un periodo de tiempo determinado (1 ó 2 días), configurar el análisis en segundo plano según la frecuencia estimada en que los usuarios acceden a elementos antiguos, y al volumen de mensajes recibidos en el intervalo de tiempo especificado.

Logs (Registros)

Esta sección permite definir la forma en que deberían ensamblarse los informes y registros de análisis de virus.
Un registro más detallado puede contener más información, pero puede afectar el rendimiento del servidor.



1. ***Log all files***
   (Registrar todos los archivos analizados)
   Si esta opción está marcada, se incluirán en el registro de análisis todos los archivos verificados, incluso aquellos que no estén infectados.

2. ***Synchronous logging***
   (Regístro inmediato)
   Cuando está marcada esta opción, todas las entradas de registro se escriben inmediatamente en el informe, sin guardarlas previamente en la memoria temporal.

3. ***Scope***
   (Alcance)
   Esta opción permite seleccionar cuál será el alcance de las actividades de registro. Cuanto más detallado sea el rango, más entradas se escribirán en el informe.

4. ***Log server version***
   (Incluir versión del servidor)
   Si está marcada esta opción, XMON escribe la versión del servidor en el informe.

5. ***Log license***
   (Incluir licencia)
   Si está marcada esta opción, XMON detalla la licencia de XMON en el informe.

6. ***Log rules***
   (Incluir reglas)
   Cuando esta opción está marcada, XMON escribe en el informe detallado la lista de reglas actualmente activas.

Configuración recomendada

Excluir los archivos de Exchange del análisis de acceso residente

XMON analiza los mensajes de correo electrónico contenidos en el almacenamiento de MS Exchange Server. Este se guarda como un archivo único en el sistema de archivos del servidor.

No utilizar la configuración estándar en el módulo de análisis de acceso AMON que se ejecuta en el mismo servidor, podría causar una seria incompatibilidad entre XMON y AMON.

Para evitar este inconveniente, asegúrese de que el módulo AMON esté configurado para excluir del análisis los archivos con extensión **.edb**, **.tmp** y **.eml**, tal como establecen los valores predeterminados.

También se recomienda excluir los directorios que contengan los siguientes archivos y carpetas:

%ProgramFiles%\Exchsrvr\MDBData

%ProgramFiles%\Exchsrvr\Mtadata

%ProgramFiles%\Exchsrvr\Server_Name.log

%ProgramFiles%\Exchsrvr\Mailroot

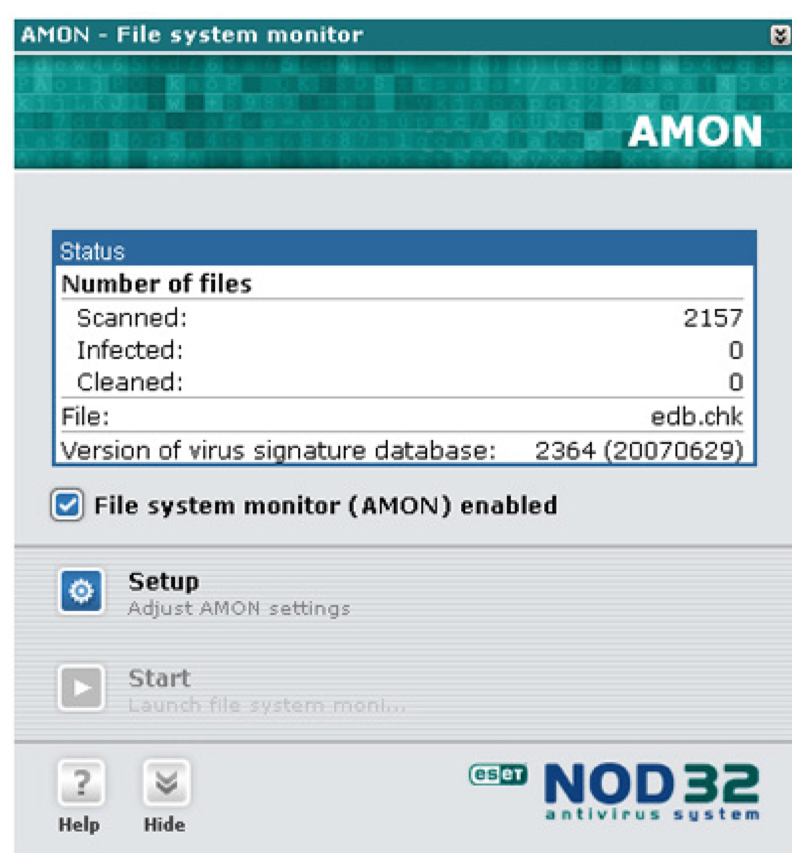
%ProgramFiles%\Exchsrvr\Srsdata

%SystemRoot%\System32\Inetsrv

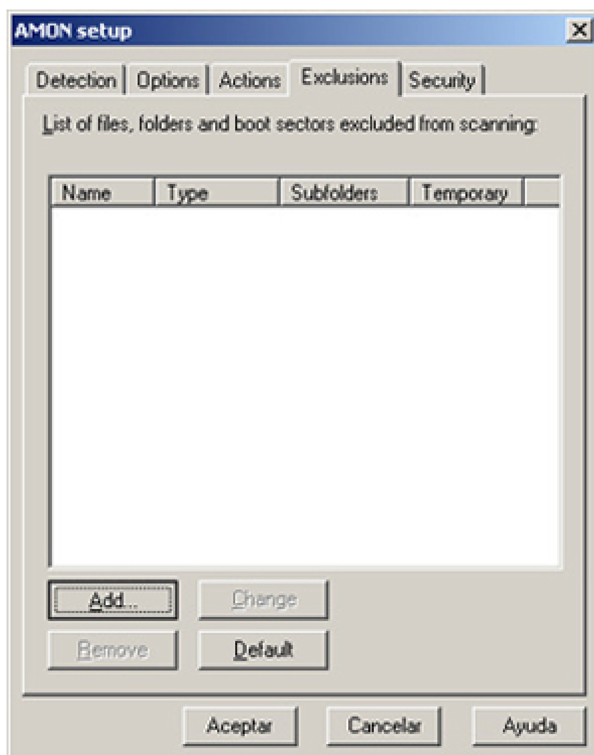
%ProgramFiles%\Exchsrvr\IMCData

Para excluir los archivos y directorios mencionados, siga las siguientes instrucciones:

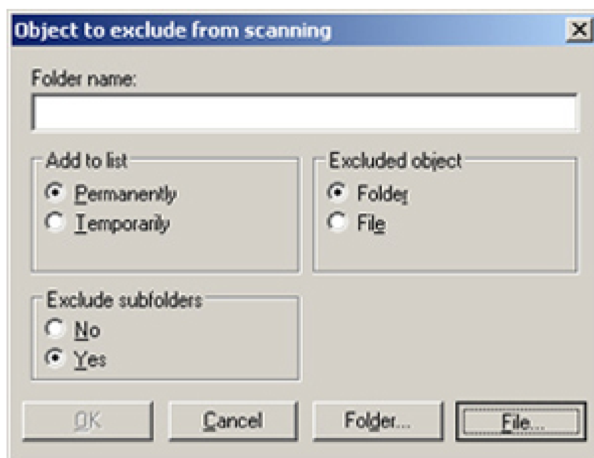
1. Abra el módulo AMON y pulse el botón ***Setup*** (Configuración).

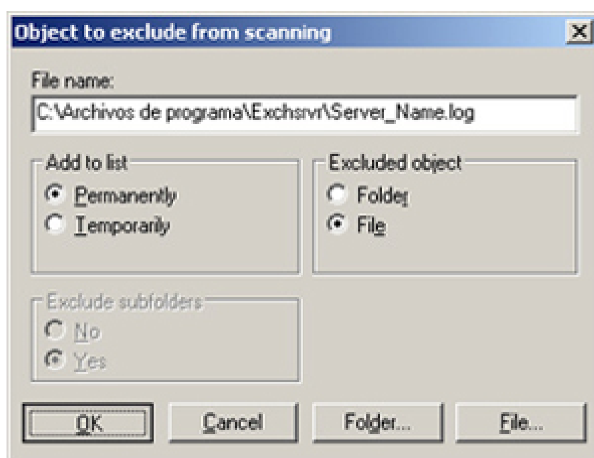


2. En la pestaña ***Exclusions*** (Exclusiones) presione el botón ***Add*** (Agregar).



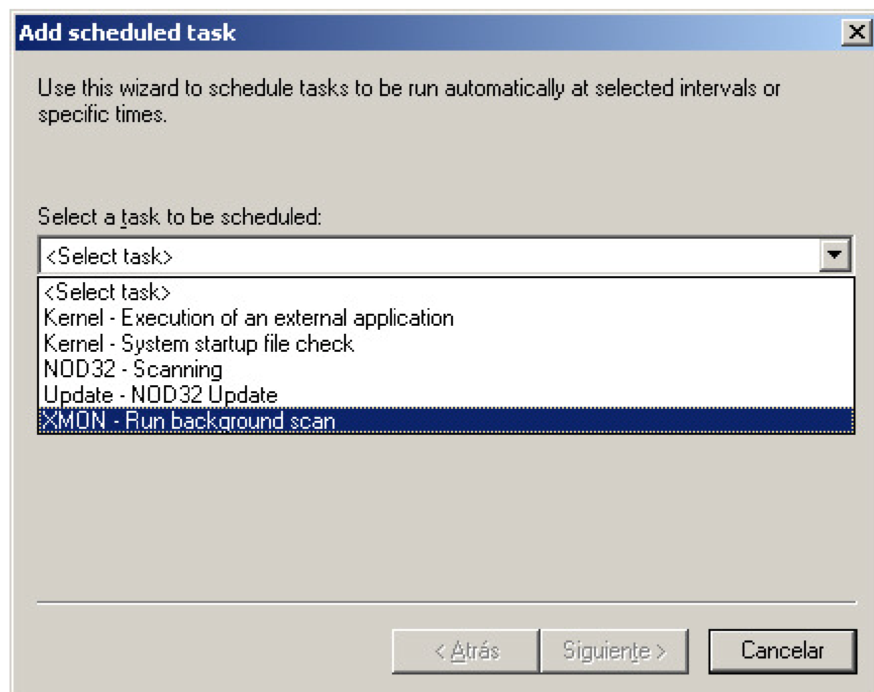
3. En la ventana que aparece, pulse el botón ***Folder*** (Carpeta) o ***File*** (Archivo), dependiendo del tipo de elemento que desea excluir. Examine la ruta hacia los ítems correspondientes.



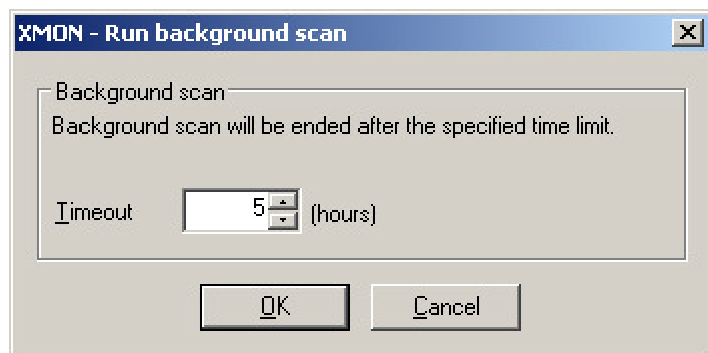


Configurar el análisis de segundo plano en el tiempo programado

El análisis en segundo plano puede configurarse utilizando una tarea especial en la sección ***Scheduler / Planner*** (Tareas programadas).
Al programar una tarea de análisis en segundo plano, se puede configurar el horario de ejecución, el número de repeticiones y otros parámetros adicionales.



El análisis en segundo plano necesita un parámetro obligatorio que especifique el límite de tiempo para la verificación. El intervalo está especificado en horas, dentro de los valores 1 a 32.

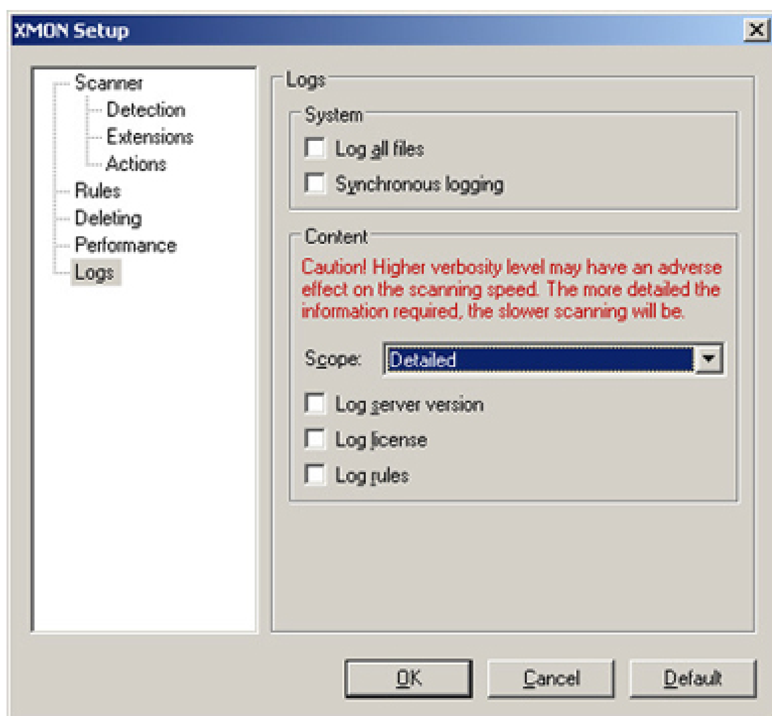


Después que la tarea ha sido definida, aparecerá en la lista de actividades programadas, y se podrán modificar sus parámetros, eliminarla o desactivarla temporalmente.
Si la tarea se ejecuta en el momento determinado, XMON permitirá que MS Exchange Server ejecute un análisis en segundo plano.
Cuando termine el tiempo límite especificado, XMON hará que MS Exchange Server finalice la verificación.
Durante este intervalo, dependerá de MS Exchange si se ejecutará un análisis en segundo plano o no, en base a varios factores, tales como la carga actual del sistema, la cantidad de usuarios activos, etc.

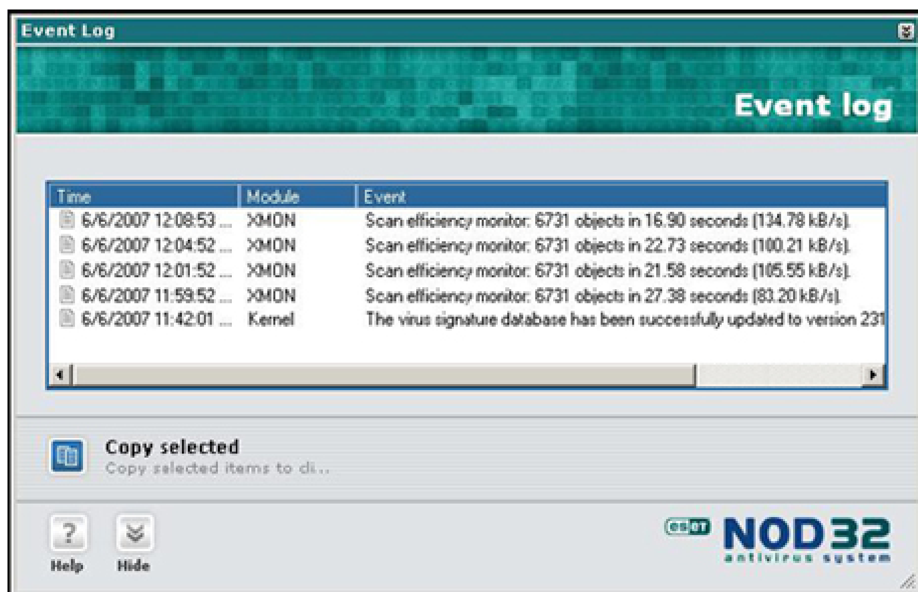
Monitorización del rendimiento

Con la transición a sistemas de 64 bits, el módulo XMON ha comenzado a utilizar un centro de control de análisis externo. Esta extensión también se aplica a la versión de 32 bits, en la cual está disponible también la opción de utilizar el centro de análisis interno.

Ambas formas de utilizar el centro de análisis tienen sus puntos a favor y en contra, dependiendo de los sistemas en los que estén instalados. Uno de los factores que los administradores tendrán que considerar al seleccionar uno de estos enfoques, es la velocidad del análisis antivirus. Para ello, desde la versión 2.71, el módulo XMON puede calcular el rendimiento actual e informarlo en el módulo de registro de eventos.
Para guardar esta información, el nivel de registros debe estar configurado en ***Detailed*** (Detallado).



Cada cinco minutos, XMON registrará información sobre el rendimiento, como la cantidad de objetos analizados (mensajes y adjuntos), tiempo de verificación en segundos, velocidad de análisis en KB por segundo, etc.



Al igual que los registros, los resultados de las monitorizaciones también se escriben en intervalos de cinco minutos. Estos no son acumulativos, y cada entrada nueva se mide desde el principio una vez que los resultados han sido guardados.

Cambiar el nombre de los archivos infectados

En las acciones a ejecutar cuando un archivo está infectado, no recomendamos marcar el valor ***Rename*** (Cambiar nombre) si se utiliza la configuración ***Scan all files*** (Analizar todos los archivos).

Todos los archivos de tipo **.exe** o **.doc** infectados tendrán, después de la modificación del nombre, la extensión **.vexe** o **vdoc**, de modo que el servidor en MS Windows se ejecutaría al pulsar sobre él.

Sin embargo, el sistema antivirus reconocerá los archivos por su contenido en cada verificación que realice, y modificará su nombre posteriormente.
Como todos los mensajes en el almacenamiento de MS Exchange Server, se analizan después de cada actualización de la base de firmas de virus, la modificación de nombres consecuente podría disminuir la velocidad del ordenador.

Se recomienda excluir del análisis al menos los archivos con extensión **.vv*** (no **.v,** porque esto incluiría también los guiones de Visual Basic).

Contacto

Soporte Técnico: ayuda@nod32-es.com

Ventas: ventas@nod32-es.com

Información general: info@nod32-es.com

ESET NOD32 en España

Ontinet.com, S.L.,
c/ Martinez Valls 56 bajos
46870 Ontinyent (Valencia)
España

Teléfono: +34 902.33.48.33

Fax: +34 96.191.03.21

ESET Central

ESET LLC
610 West Ash Street, Suite 1900
San Diego, CA 92101
U.S.A.

Teléfono: +1 (619) 876.5400

Fax: +1 (619) 437-7045